

UNITED STATES DISTRICT COURT
for the
Eastern District of Wisconsin

United States of America

v.

JUN XIE

Case No.

14-M-459

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

Between in or around March 2014, and in or around June 2014, in the state and Eastern District of Wisconsin, and elsewhere, the defendant violated:

Code Section

Title 18, United States Code,
Section 1832(a)(1) and (2)


Offense Description

Theft of Trade Secrets

This criminal complaint is based on these facts:

See Attached Affidavit

☒ Continued on the attached sheet.



Complainant's signature

Gerald Shinneman, FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date:

September 3, 2014



Judge's signature

City and state:

William E. Callahan Jr., U.S. Magistrate Judge

Printed name and title

AFFIDAVIT

I, Gerald Shinneman, being duly sworn, state as follows:

1. I am a Special Agent assigned to the Milwaukee Field Office of the Federal Bureau of Investigation. I have been a Special Agent with the FBI since January 2002. I have received specialized training and participated in investigation involving violations of federal criminal laws and regulations, including economic espionage and theft of trade secrets.

2. This affidavit is made in support of an application for a criminal complaint charging that JUN XIE ("XIE") did knowingly steal, or without authorization appropriate, take, carry away or copy, duplicate, download, and replicate a trade secret that is related to or included in a product that is produced or placed in interstate or foreign commerce, for the economic benefit of anyone other than the owner of the trade secret, intending or knowing that the offense will injure any owner of that trade secret, in violation of Title 18, United States Code, Section 1832(a)(1) and (2).

3. The information in this affidavit is based upon my personal knowledge, my review of documents, and information from other law enforcement agents and persons with knowledge regarding relevant facts. Because this affidavit is submitted for the limited purpose of obtaining a criminal complaint and arrest warrant, I have not included each and every detail that I have learned during this investigation. I have set forth only those facts that I believe are necessary to establish probable cause for the criminal complaint and arrest warrant.

FACTS SUPPORTING PROBABLE CAUSE

4. According to U.S. immigration records, XIE is a citizen of China and he is residing in the United States under an H1B non-immigrant work visa. XIE has lived in the United States since 2002.

5. GE Healthcare (“GEHC”) is a unit of General Electric Company (“GE”), with an office in the Eastern District of Wisconsin. GEHC offers a broad range of products, including magnetic resonance (“MR”) systems that are sold in interstate and foreign commerce.

6. According to a representative for GEHC, XIE was an employee of GE Medical Systems LLC, a wholly owned subsidiary of GEHC and GE. XIE was hired in 2008 as a “Pulse Sequence Diagram Applications Engineer.” In his position, XIE was responsible for writing and creating source code and computer programming for MR technology used in systems in current production and those in development.¹

7. According to a representative for GEHC, between in or around March 2014 and in or around June 2014, GE detected that XIE downloaded and copied approximately 2.4 million GEHC-owned electronic files (1,468 gigabytes) from GEHC’s computer network without authorization. Included in the material downloaded and copied by XIE were engineering designs, product testing data, business and product strategy information, and source code for operating GEHC’s MR systems.

8. On or about June 9, 2014, based XIE’s downloading activity from GEHC, the FBI interviewed XIE at his residence in Waukesha, Wisconsin. Before the interview, the agents

¹ As used in this affidavit, “source code” means computer programming instructions in their original form.

advised XIE of his rights under *Miranda* in both English and Mandarin. XIE acknowledged that he understood his rights and agreed to waive those rights. During the interview, XIE stated the following:

(a) In early 2013, XIE's wife moved from the United States to China. At that time, XIE knew he would eventually move back to China and obtain employment there. It was around that same approximate time that XIE began downloading GEHC-owned documents and files from GEHC's computer network.

(b) XIE located documents and files to download from GEHC's computer network utilizing a word search function on the network. XIE reviewed documents produced from the word search; and he download documents and files that he thought might be useful to him in the future. If the word search produced too many results for XIE to review, XIE downloaded all of files without reviewing them. XIE claimed that he was unaware of the specific content of what he was downloading when he downloaded large result sets. XIE stated that he knew some of the documents he downloaded were very important to GEHC, and that those documents must never be given to anyone. XIE considered deleting those documents from the downloaded results, but he did not. XIE claimed that he never noticed that the downloaded documents were marked "Proprietary."

(c) XIE downloaded GEHC-owned documents and files to his GEHC issued computer and several personal removable electronic storage devices. XIE sent the downloaded GEHC documents, files, and information to family members located in China on four separate removable electronic storage devices. XIE sent two one-terabyte size hard drives to his wife in Guangzhou, China; and he sent the other two one-terabyte size hard drives to his brother in

Fuzhou, China. XIE did not believe the four separate one-terabyte hard drives were full, but he did not know how much GEHC information was contained on each storage device.²

(d) In or around March 2014, XIE submitted his resume to a Chinese imaging company (the "Chinese Company"), located in China. In April or May 2014, XIE interviewed with the Chinese Company. A short time later, the Chinese Company offered XIE a position as a magnetic resonance engineer. XIE's anticipated start date with the Chinese Company was July 25, 2014.

(e) XIE intended to use the GEHC downloaded information for his personal use and benefit when he returned to China. XIE acknowledged that he could use the GEHC owned information in a future magnetic resonance engineering job. XIE claimed that he never provided any GEHC documents to the Chinese Company and that he never intended to provide any GEHC documents to the Chinese Company. XIE indicated that he may have discussed some GEHC technologies in the cardiology field with the Chinese Company during one of his interviews, but he did not tell them it was GEHC-owned technology.

9. According to law enforcement reporting and conversations with GEHC representatives, the Chinese Company competes with GEHC in the MR field.

10. According to GEHC representatives, GEHC maintains several security measures to insure confidentiality of its trade secret and proprietary information. GEHC is a secured facility and that can be accessed only with an employee identification badge.

11. According to the Chief Information Security Officer for GEHC, each GEHC employee is provided an employee identification badge that is comprised of his/her name and

²The electronic storage devices used by XIE have been recovered from China and they are being analyzed.

employee credential number. The identification badge acts as a key card, and GEHC employees must use the identification badge to gain access to the GEHC facility in Wisconsin. GEHC employees must use the employee credential number and a unique password, created by the employee, to access GEHC's computer network, which houses GEHC trade secret and proprietary information. Also, GEHC employees may require additional grants of access authorization to gain access to certain areas within the GEHC computer network.

12. Additionally, when GEHC employees use an encrypted GEHC-owned laptop, a warning banner is displayed on the screen that notifies the user that use of the computer and network is "allowed for legitimate purposes only and in accordance with GE Policies and Guidelines." According to the Chief Information Security Officer for GEHC, XIE used a GE-issued encrypted laptop that displayed the warning banner when accessed and downloaded the GEHC-owned information.

13. GEHC also has in place a series of company policies and regulations, as well as confidentiality and non-disclosure agreements with employees and third-parties, in order to protect its trade secrets and other proprietary information. According to a representative for GEHC, XIE signed a confidentiality and non-disclosure agreement, known as the Employee Innovation and Proprietary Information Agreement ("EPIA"), when he started his employment with GEHC. Under the EPIA, XIE was prohibited from "us[ing], publish[ing] or otherwise disclos[ing] . . . subsequent to [his] employment, any secret or confidential information or data of [GEHC]." The EPIA defined "secret" and "confidential" as follows:

[GEHC] generally considers "secret" or "confidential" any information or data that is not generally known - regardless of whether such information or data is in oral, written, machine readable or other form. When in doubt, you should assume that information or data is secret or confidential unless or until determined

otherwise. Without limitation, examples of information or data that may be of a secret or confidential nature are: drawings, manuals, notebooks, reports, models, inventions, formulas, processes, machines, compositions, computer programs, accounting methods, business plans, information systems, customer and employee lists and any information and data in electronic form.

14. According to the Chief Information Security Officer for GEHC, XIE had extensive access to the GEHC proprietary and trade secret information stored on its internal password protected network due to his position as a Pulse Sequence Diagram Applications Engineer. XIE used his access to locate and download numerous GEHC-owned trade secret and proprietary materials from certain areas on the GEHC computer network. Each of these areas on the internal GEHC network maintained an additional level of access control.

15. Although GEHC continues to assess the full scope of XIE's unauthorized downloading activities, based on the investigation to date, GEHC determined that XIE took propriety and trade secret information and the disclosure of that information to the public would cause irreparable injury to GEHC.³ For example, in addition to source code and other

³On or about July 11, 2014, GE filed a civil complaint against XIE in the U.S. District Court for the Eastern District of Wisconsin. The matter was assigned case number 14-CV-809. In the complaint, paragraph 33, GE more specifically described the types of information XIE downloaded. In the civil complaint, GE stated:

Among these trade secrets are confidential GEHC documents constituting or reflecting: images of data from GE's actual MR machines; MR source code, test vectors, and documentation covering GE image reconstruction and pulse sequencing algorithms; modeling techniques and optimizations for components of GE MR products; MR engineering design approaches and implementations; MR product and system architecture, technical features, and components; MR business strategy; MR product performance data; GEHC product plans from its CT, Vascular and Mammography businesses, including associated development costs; presentations which lay out GE's 3-year prospective outlook relating to such key metrics as MRI market size, and intra-market competitive trends, GE product planning, technology opportunities, business costs, and business profitability for current MR projects; hardware development of GE's MR PET product, including system development technical risks and technical specifications, and design strategies); test data and results for specific MR Product programs; technical notes, research reports, source code, and engineer tool descriptions

proprietary information, GEHC determined that XIE downloaded a document titled "Silent MR Roadmap," which contained business strategy information related to "silent" MR technology and competitor information in that field. Another file XIE downloaded was titled "GPB 2010 MR." According to a GEHC representative, "GPB" is an acronym for "Growth Play Book" and the document XIE downloaded contained information related to MR product projections and an assessment of domestic and international MR competitors.

CONCLUSION

16. Based on the above information, I respectfully submit that there is probable cause to believe that XIE did knowingly steal, or without authorization appropriate, take, carry away or copy, duplicate, download, and replicate a trade secret that is related to or included in a product that is produced or placed in interstate or foreign commerce, for the economic benefit of anyone other than the owner of the trade secret, intending or knowing that the offense will injure any owner of that trade secret.

generated by GEHC's Applied Science Laboratory; Advanced Technology Project Reports from 2012-2013 that cover a wide array of confidential and proprietary hardware, systems, coils, and software applications developments; and Overall Project Status Reviews which detail program execution status, key technical decisions, timing, and costs for numerous current GEHC projects.